BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

Eur päisches Patentamt	Eur pean Patent Office	Office ur péen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

00480027.2

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 18/04/00
LA HAYE, LE

Eur päisches Patentamt
Eur pean Patent Office
Office eur péen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 00480027.2

Anmeldetag:
Date of filing:
Date de dépôt: 20/03/00

Anmelder:
Applicant(s):
Demandeur(s):
International Business Machines Corporation
Armonk, N.Y. 10504
UNITED STATES OF AMERICA

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Data transmission system for reserving a virtual connection in an IP network equipped with a reservation server

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

DATA TRANSMISSION SYSTEM FOR RESERVING A VIRTUAL CONNECTION IN AN IP NETWORK EQUIPPED WITH A RESERVATION SERVER

Technical field

The invention relates to the reservation of virtual connections with a Quality of Service in an IP network and relates in particular to a system and a method for the reservation of virtual connection in such a network equipped with a reservation server.

Background

In any transmission wherein a connection is first established before the transmission takes place, bandwidth is reserved along the path used by the connection and error checking is taken into consideration along the path. The protocols using such an approach use a call-connect packet to initiate a session and a connect-confirm response packet to complete the call sequence.

The requirements of connection-oriented systems are that the route is determined at call set up time by allocating a virtual circuit between the two endpoints. At that time, all necessary resources on the virtual circuit are reserved and logical channels are allocated. It is only when the connection is cleared that the resources and logical channels are released.

For example, with Asynchronous Transfer Mode (ATM) networks, a call set up process is established using virtual paths/virtual circuits (VP/VC). All ATM communications are set up by using a controlled method which identifies the rights needed to establish each connection. Generally, connections are not established by end users but by the network devices or nodes. However, there is a trend today to use packet-switched telecommunications directly at IP (Internet Protocol) level which allows the end-users to establish directly the connections.

A connectionless transmission used for example at IP level, is a form of packet-transmission not requiring communications between the end devices before the transmission of data and therefore, is well-adapted to transmit short messages composed of or limited number of packets. Therefore, it is a data transfer without the use of virtual circuit. In simple bus or ring networks, there is no problem implementing connectionless systems because the path-choice is limited. However in meshed and complex networks, the problems are significantly different. Each router must have a large amount of intelligence to process the packet header, and the network requires an efficient mechanism to ensure that all routers or nodes have an up-to-date view of the overall topology.

The Resource Reservation Protocol (RSVP) is a network-control protocol that enables IP applications to obtain special Qualities of Service (QoS) for their data flows. It allows to

establish connection-oriented like communications with quality of service. But RSVP is not a routing protocol. Instead, it works in conjunction with routing protocols and installs the equivalent of dynamic access lists along the routes that routing protocols calculate. RSVP can be used by end-users to reserve bandwidth on the pass to the destination on all involved routers. The limitation is that if the bandwidth is already used, there is no way to add more reserved communications. No control on the rights of the end-user to ask for bandwidth is provided.

Another difficulty with a current reservation protocol such as RSVP is that there is not enough scalability since each request has to be handled by each network device or node in the path used by the connection.

Summary of the invention

Accordingly, the main object of the invention is to provide a data transmission system for transmitting packets of data through an IP network equipped with a reservation server capable of setting up a virtual connection with a Quality of Service from a source workstation to a destination workstation.

Another object of the invention is to achieve a method for reserving a virtual connection for performing secure and controlled resource reservation in an IP network and in particular for checking the user rights and providing an identification to the flow established between a requesting source workstation and a destination workstation.

The invention relates therefore to a data transmission system for transmitting packets of data from a source workstation to a destination workstation wherein the packets of data are transmitted over an IP network between an ingress node

connected to the source workstation and an egress node connected to the destination workstation. The system comprises a reservation server accessible by the source workstation and including connection setup means for setting up a virtual connection meeting a predefined requirement of Quality of Service from the ingress node to the egress node in response to a request from the source workstation.

The invention relates also to a method for reserving a virtual connection by a source workstation using the above system comprising the steps of sending a reservation request from the source workstation to the reservation server, checking that the request may be validated in view of information about the user of the source workstation accessible by the reservation server, verifying that the capacity of the IP network enables to meet the requirements of the request, and setting up a virtual connection from the ingress node to the egress node when the capacity of the IP network enables to meet the request requirements.

Brief description of the drawings

The above and other objects, features and advantages of the invention will be better understood by reading the following more particular description of the invention in conjunction with the accompanying drawings wherein :

-Fig. 1 represents a block diagram of a data transmission system wherein an IP network is equipped with a reservation server according to the principles of the invention.

-Fig. 2 is a flow chart representing the steps of the virtual connection reservation in a requesting source workstation.

-Fig. 3 is a flow chart representing the steps performed in the reservation server when receiving a reservation request from a source workstation.

-Fig. 4 is a flow chart representing the steps performed in a source workstation after receiving the reservation message from the reservation server.

-Fig. 5 is a flow chart representing the steps performed in an edge node after receiving the information about a reservation from the reservation server.

-Fig. 6 is a flow chart representing the steps performed by the ingress edge node when receiving the frames from the source workstation.

Detailed description of the invention

In reference to Fig. 1, a data transmission system according to the invention can include a source workstation 10 attached to a LAN 12 and which may access to an IP network 14 through a default router 16. This one is connected physically to several edge devices such as edge nodes 18 or 20 which are themselves connected to edge nodes 22 or 24 though IP network 14. A reservation server 26 according to the invention may be accessed by any workstation such as the source workstation 10 through several intermediary nodes such as backbone nodes 28 and 30. When a source workstation 10 wants to send data packets to another workstation such as destination workstation 32, a virtual connection through backbone nodes such as backbone node 34 is established by reservation server 26 between source workstation 10 and destination workstation 32.

Of course, source workstation 10 may use the IP network in a non reserved mode as usual. But, according to the invention, it may request a reservation to the reservation server when needed by some applications requiring a Quality of Service (QoS.). Such a reservation may be a direct reservation to the reservation server or a generic reservation forwarded by default router 16 to reservation server 26. The reservation server performs the user authentication and checks if the reservation can be granted to this user. If so, the edge nodes

involved in the connection such as nodes 20 and 24 are informed of the new reserved flow. In parallel, the requesting workstation 10 is informed that it can proceed to the communication. A flow identification may be provided to speed up the recognition and validation of that flow at the ingress node 20.

Fig. 2 is a flow chart representing the steps of making a resource reservation from source workstation 10. When a user of source workstation 10 needs a new reservation (step 40) which can be a manual reservation or a reservation requested by an upper application, a reservation request message is built (step 42) including the necessary parameters such as destination, bandwidth, Quality of Service, type protocol or port number. A duration may also be provided or an indication that the reservation is valid until a cancellation message is sent to the reservation server. Note that a reservation request message can also be built when the workstation receives new parameters from said reservation server because the request from the source workstation cannot be accepted as explained below in reference to Fig. 4. Once the reservation request message is ready, it is sent (step 44) to the reservation server. The message is of course followed by a classical authentication sequence as explained in reference to Fig. 3.

The steps performed in reservation server 26 when a request is sent by source workstation 10 are presented in Fig. 3. After receiving the request (step 46), the server starts a user authentication (step 48) which can be a LogonID/password verification or a more sophisticated authentication using certificates. This verification involves the use of a data base 50 storing the identification of each user and the user/customer profile when the user of the source workstation is one of a plurality of users associated with a customer of the server. Then, a user rights verification (step 52) is

performed using the same data base 50 which defines for each user which kind of request he is allowed to perform. The result of such a verification may be in terms of bandwidth required for a call, destination allowed, Quality of Service... As the reservation results in an extra cost for the customer based on the type and duration of the communication to be performed, it is important to offer a way for the customer to manage the authorization for each user being authorized by the customer. If the verification of the user rights fails, the request is rejected with a rejection message (not shown) sent to the workstation including a code for the rejection.

If the request is validated, the process checks the network capability (step 54) for this request. For that, the process uses a network data base 56 which is used to know the remaining capacity of each link in the network. The capacity requested for setting up a virtual connection from ingress node 20 to egress node 24 has to meet Quality of Service parameters within the network. After checking whether the network capacity is sufficient (step 58), a new capability has to be set (step 60) for being proposed to the workstation if it is not the case. In such a case, this new capability may be either a lower bandwidth or a lower Quality of Service, which is then sent back to the requesting workstation (step 62). At the same time, an updating message is transmitted to the edge nodes as explained later in reference to Fig. 5.

If the network is able to support the request of the workstation, a flow identification is set (step 64). Such a flow identification includes not only a FlowID field but also the parameters such as source address, destination address, Quality of Services, port number, duration, bandwidth, route or path within the network. Some of these information are used to update network data base 56 such as bandwidth, duration, Quality of Services (step 66) and an answer including the

acceptance for the request is sent to the requesting workstation (step 62). Note that some parameters such as source address, destination address, port number, route or path within the network and also Quality of Service are sent to the edge nodes of the virtual connection as explained later in reference to Fig. 5.

The steps performed in the user workstation after the processing of the workstation request by the reservation server are illustrated in Fig. 3. After receiving the reservation answer message from the server (step 70), a test is done (step 72) as to whether it is an accepted request confirmation or a new proposal from the server since the request may not be totally fulfilled as explained in reference to Fig. 3. When the request has not been accepted, new parameters are proposed by the reservation server and a test is whether such parameters are acceptable by the user of the workstation (step 74). If so, a new reservation request message is built as explained in reference to Fig. 2. If the new parameters are not accepted, this means that the request can be considered as being aborted (step 76).

When the request has been accepted by the reservation server, the workstation gets a flow identification defined by a FlowID (step 78) that the user will use within each frame header to identify the flow to which the frame belongs. Such a FlowID may be a flow label used within IP version 6 (IPv6) or a MPLS label or any identification field within the protocol used by the workstation to communicate with the ingress node. Note that the flow identification is the preferred embodiment but could be bypassed when IP version 4 (IPv4) is used natively and results in a more complicated identification on the ingress node port.

After getting a flow identification or FlowID, a data base 80 storing the user FlowIDs to the purpose of being used for

local accounting is updated (step 82). Then, the user application is informed of the FlowID (step 84) and may start sending the frames of the flow (step 86).

As explained above in reference to Fig. 3, an updating message is transmitted to the edge nodes by the reservation server after the capacity of the network to fulfill the request has been checked. As illustrated in Fig. 5, this message received by the edge nodes (step 88) is used for updating. Note that, edge nodes are the ingress node 20 (see Fig. 1) which receives the data frames from the source workstation and the egress node 24 which receives the data frames from the ingress node through the IP network. The data frames are identified either by the FlowID set by the reservation server or by a route identification defined by a RouteID which has been substituted to the FlowID by the ingress node. Such a substitution is provided by the reservation server either to both ingress node and egress node or only to the ingress node. The information may be the identification of a already known route or all information needed to define a new route. It must be noted that, when the information about the route is sent only to the ingress node, it is necessary to transmit a complete header within each frame of the flow, whereas some data fields such as the source address, the destination address, the port number and the Quality of Service are not transmitted within the frame header when the information is transmitted to both ingress and egress nodes.

Note also that, when a substitution from FlowID to a RouteID occurs, not only the FlowID field is changed but also fields such as Quality of Service or the type of service (ToS). The objective is to rebuild the same frame at the output of the egress node as the frame at the input of the ingress node, even if some fields are changed within the network except fields such as Time To Live (TTL) which needs always to be decremented. Further to replace the FlowID by a RouteID, it

may be useful in the case where two networks are used, to replace the FlowID corresponding to the first network by a new FlowID corresponding to the second network, the value of this new FlowID being given by the reservation server of the second network to the egress node of the first network. Coming back to Fig. 5, the update message received from the reservation server is used to update (step 90) a data base 92 storing the FlowIDs. The stored information will be used only when a frame is received at the interface of the ingress node as illustrated in Fig. 6.

When a new frame is received by the ingress node (step 94), the interface process first performs a lookup (step 96) in its local port forwarding data base 98 to check whether the flow to which belongs the received frame is a known flow or a new one (step 100). If it is a known flow, the frame is processed and modified (step 102) before being forwarded (step 104). For example, non-reserved flows may be forwarded with minor changes such as only TTL decrementation Likewise/reserved flows may have a new Quality of Service classification and a new identification field. Even some fields such as source address and destination address may be removed if the identification field with the network is unique when the egress node has been informed by the reservation server and is able to put back these address fields within the frame.

When the received frame corresponds to a new flow, there is a FlowID verification (step 106) by comparing the FlowID to reserved flows stored in data base 92 as explained in Fig. 5. When the flow corresponds to an existing flow in the data base, the Quality of Service of the flow is set (step 108) and an update of the port forwarding data base 98 is performed in order to find and process directly the subsequent frames of this flow (step 96). The frame is then processed and modified (step 102) before being transmitted (step 104). In addition, the reservation server is informed that a first frame of a new

flow has been received and processed which will start a connection timer for this flow for accounting of the use of this reservation. Note that, when the flow is not recognized as a reserved flow (step 106), the frame is processed as a non-reserved flow. In this case, in order to verify that the FlowID is valid, not only the existence of the FlowID is verified, but also the source and destination addresses are checked with the port number. The FlowID and the other above listed IP header parameters are compared to the information given by reservation server 26 to ingress node 20 for this flow. This verification prevents non-authorized users to reserve bandwidth on the network just by using random FLowIDs as they will never be sent to destination.

CLAIMS

1. Data transmission system for transmitting packets of data from a source workstation (10) to a destination workstation (32) wherein said packets of data are transmitted over an IP network (14) between an ingress node (20) connected to said source workstation and an egress node (24) connected to said destination workstation ;

said system being characterized in that it comprises a reservation server (26) accessible by said source workstation including connection setup means for setting up a virtual connection meeting a predefined requirement of Quality of Service from said ingress node to said egress node in response to a request from said source workstation.

2. Data transmission system according to claim 1, wherein said reservation server (26) includes a user data base (50) for storing the identification of each user allowed to access said reservation server.

3. Data transmission system according to claim 2, wherein said data base (50) is also used for storing the rights of each user allowed to access said reservation server (26).

4. Data transmission system according to claims 1, 2 or 3 wherein said reservation server (26) further includes a network data base (56) for storing the information about the capacity of said network (14) required to set up said virtual connection.

5. Data transmission system according to any one of claims 1 to 4, wherein said source workstation includes a user FlowID data base (80) for storing the FlowIDs identifying the flows transmitted from said workstation (10).

6. Data transmission system according to any one of claims 1 to 5, wherein said ingress node (20) includes an edge FlowID data base (92) for storing the FlowIDs of the flows which have been reserved by said reservation server (26).

7. Data transmission system according to any one of claims 1 to 6, wherein said ingress node (20) includes a port forwarding data base (98) for storing the information necessary to said ingress node when receiving a first frame of a flow which has been reserved by said reservation server (26).

8. Method for reserving a virtual connection by a source workstation (10) using a system according to claim 1, comprising the steps of sending a reservation request from said source workstation to said reservation server (26), checking that said request may be validated in view of information about the user of said source workstation accessible by said reservation server, verifying that the capacity of said IP network (14) enables to meet the requirements of said request, and setting up a virtual connection from said ingress node (20) to said egress node (24) when the capacity of said IP network enables to meet the request requirements.

9. Method according to claim 8, wherein said step of checking that said request may be validated consists in checking the authentication of said user and verifying the user rights to get said virtual connection.

10. Method according to claim 8 or 9, wherein a new reservation request is sent from said source workstation (10) to said reservation server (26) if the capacity of said IP network (14) does not enable to meet the requirements of the previous request, said new request being based upon new

parameters taking the capacity of said network into account which are provided by said reservation server to said source workstation.

11. Method according to claims 8, 9 or 10, further comprising the step of sending from said reservation server (26) to said ingress (20) and egress (24) nodes all information required to set up a virtual connection from said ingress node to said egress node and a flow identification of the communication to be established so that said ingress node be able to transmit on said connection any frame of packets received from said source workstation (10).

12. Method according to claim 11, wherein the information sent by said reservation server (26) to said ingress (20) and egress (24) nodes to set up a virtual connection includes a FlowID identifying the flow corresponding to the communication to be established over said virtual connection.

13. Method according to claim 12 wherein the frame FlowID of a new frame received by said ingress node (20) is compared with the FlowIDs corresponding to reserved virtual connections which have been sent from said reservation server (26) to said ingress node (20).

14. Method according to claim 12 or 13, wherein said reservation server (26) sends a RouteID rather than said FlowID to said ingress (20) and egress (24) nodes, said RouteID identifying a route already known by said nodes.

15. Method according to any one of claims 11 to 14, wherein said information required to set up a virtual connection is only sent to said ingress node (20), the header of all frames belonging to the flow using said virtual connection

containing in such a case all the information necessary for said egress node (24) to identify said flow such as the source address, the destination address, the port number and the Quality of Service.

16. System comprising means adapted for carrying out the steps of the method according to any one of claims 8 to 15.

DATA TRANSMISSION SYSTEM FOR RESERVING A VIRTUAL CONNECTION IN AN IP NETWORK EQUIPPED WITH A RESERVATION SERVER

Abstract

Data transmission system for transmitting packets of data from a source workstation (10) to a destination workstation (32) wherein the packets of data are transmitted over an IP network (14) between an ingress node (20) connected to the source workstation and an egress node (24) connected to the destination workstation. The system is characterized in that it comprises a reservation server (26) accessible by the source workstation including connection setup means for setting up a virtual connection meeting a predefined requirement of Quality of Service from the ingress node to the egress node in response to a request from the source workstation.

FIG. 1

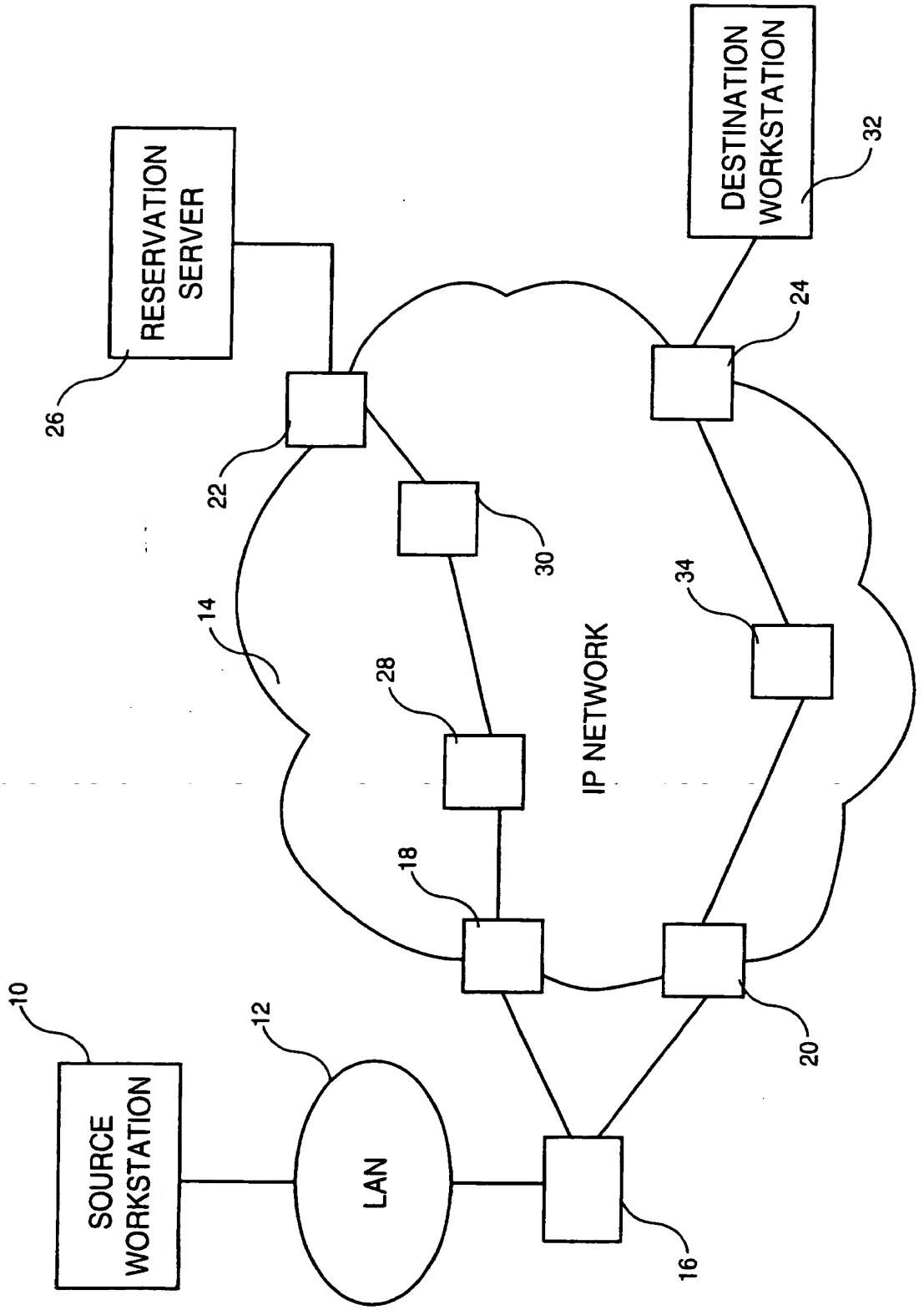
RESERVATION SERVER
26
DESTINATION WORKSTATION
32
22
24
30
34
14
28
IP NETWORK
18
20
10
12
SOURCE WORKSTATION
LAN
16

FIG. 1

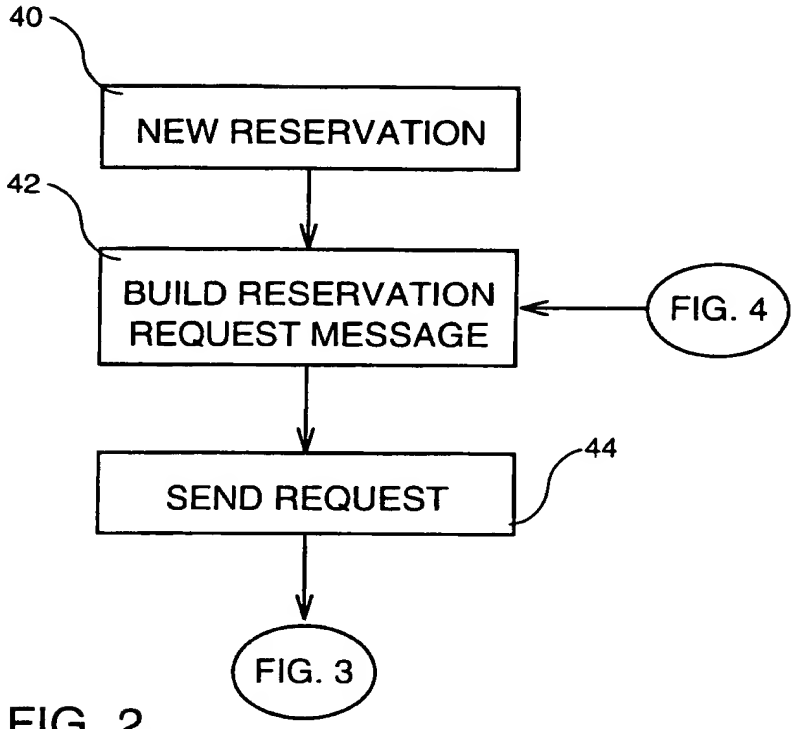
40
NEW RESERVATION
42
BUILD RESERVATION REQUEST MESSAGE
FIG. 4
SEND REQUEST
44
FIG. 3

FIG. 2

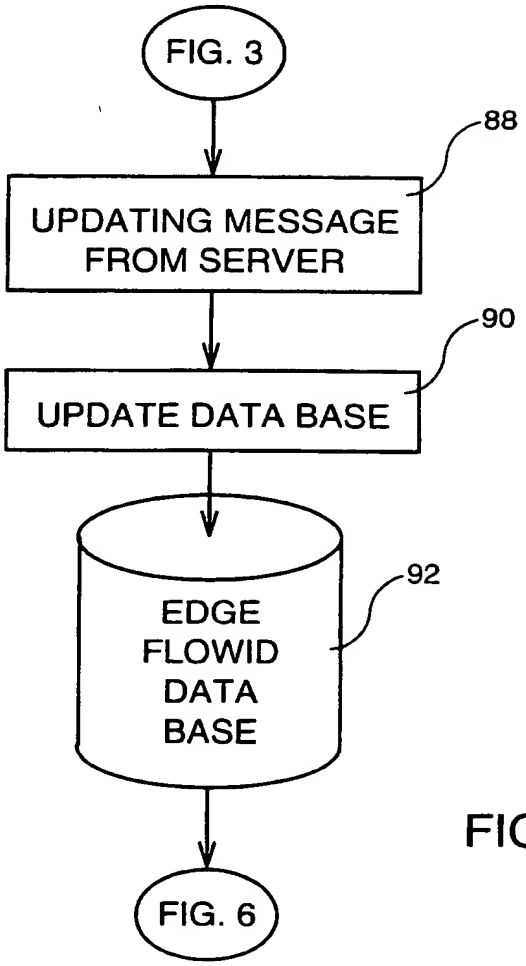
FIG. 3
88
UPDATING MESSAGE FROM SERVER
90
UPDATE DATA BASE
92
EDGE FLOWID DATA BASE
FIG. 6

FIG. 5

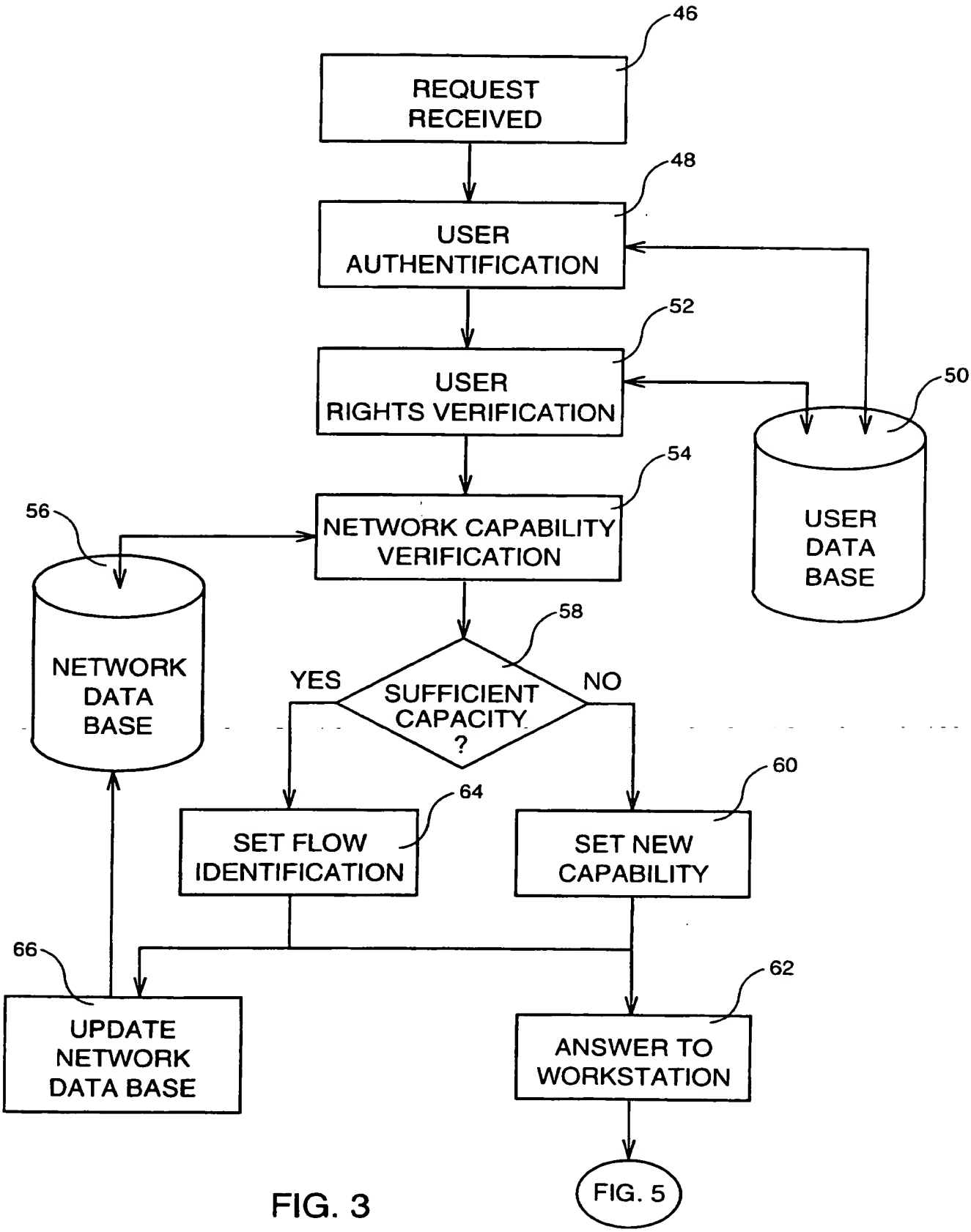
46
REQUEST RECEIVED
48
USER AUTHENTIFICATION
52
USER RIGHTS VERIFICATION
50
USER DATA BASE
54
NETWORK CAPABILITY VERIFICATION
56
NETWORK DATA BASE
58
YES
SUFFICIENT CAPACITY ?
NO
64
SET FLOW IDENTIFICATION
60
SET NEW CAPABILITY
66
UPDATE NETWORK DATA BASE
62
ANSWER TO WORKSTATION
FIG. 5

FIG. 3

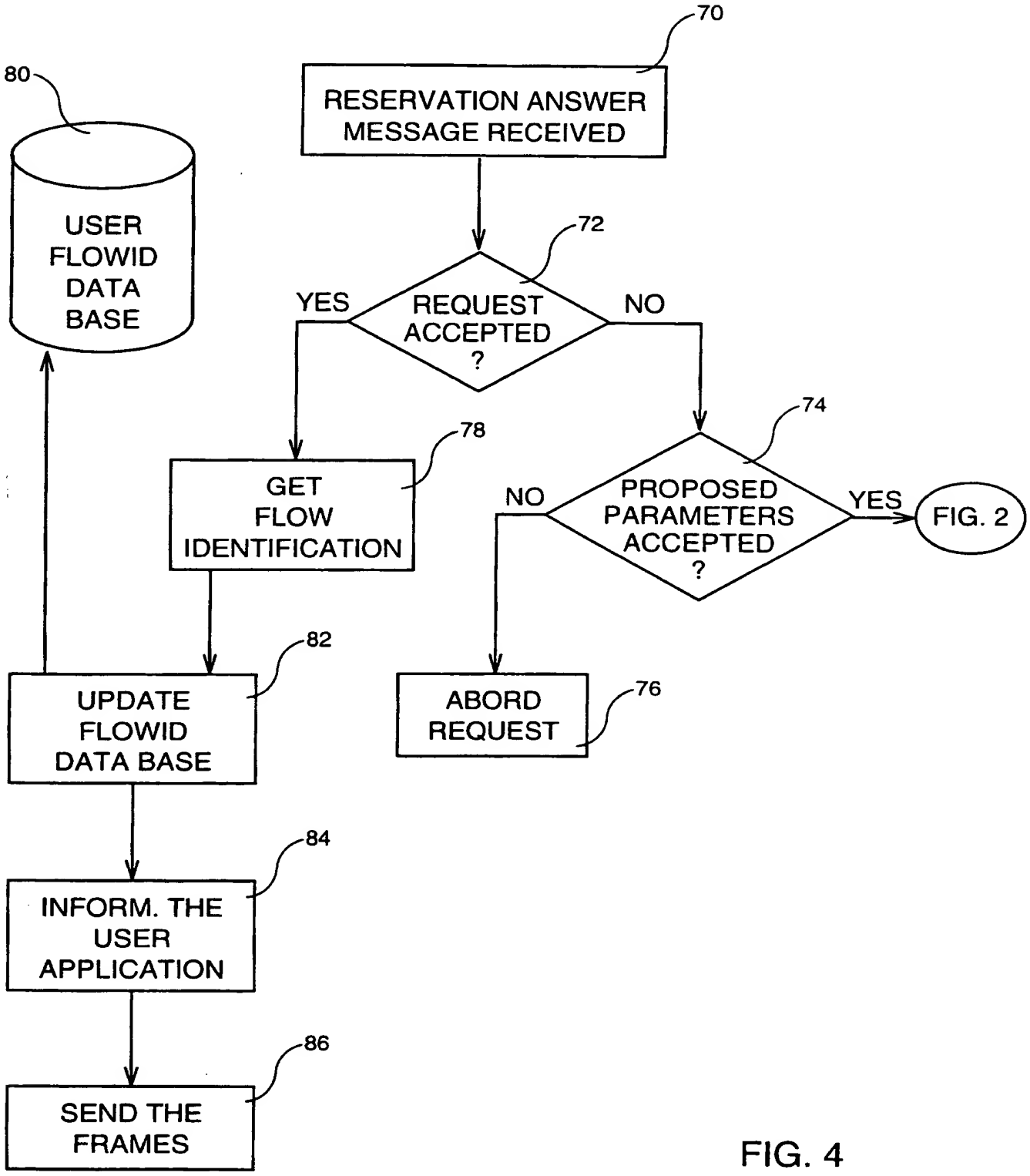
70
RESERVATION ANSWER MESSAGE RECEIVED
80
USER FLOWID DATA BASE
72
REQUEST ACCEPTED ?
YES
NO
74
PROPOSED PARAMETERS ACCEPTED ?
NO
YES
FIG. 2
78
GET FLOW IDENTIFICATION
82
UPDATE FLOWID DATA BASE
ABORD REQUEST
76
84
INFORM. THE USER APPLICATION
86
SEND THE FRAMES

FIG. 4

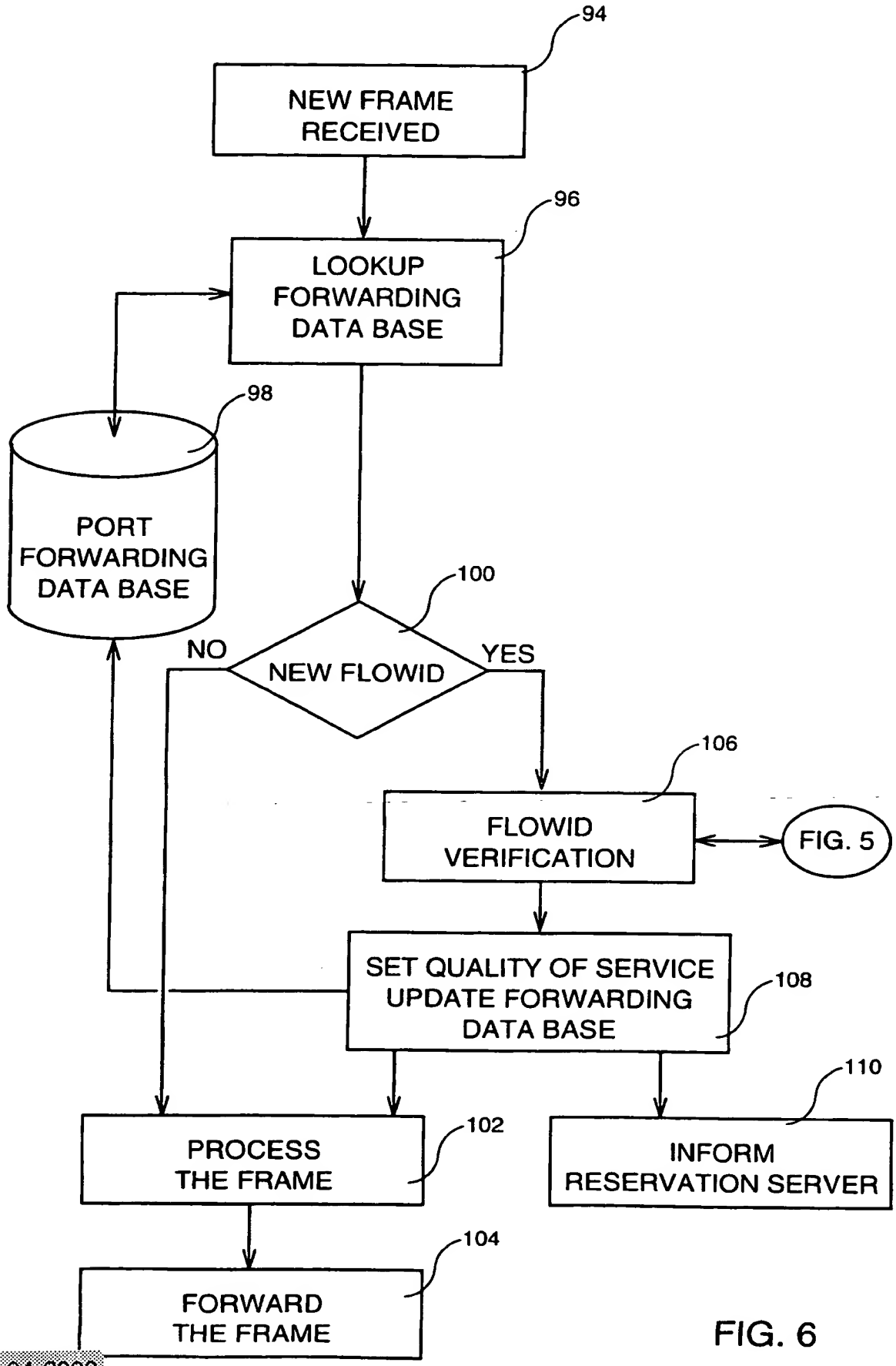
94
NEW FRAME RECEIVED
96
LOOKUP FORWARDING DATA BASE
98
PORT FORWARDING DATA BASE
100
NEW FLOWID
NO
YES
106
FLOWID VERIFICATION
FIG. 5
SET QUALITY OF SERVICE UPDATE FORWARDING DATA BASE
108
110
INFORM RESERVATION SERVER
102
PROCESS THE FRAME
104
FORWARD THE FRAME

FIG. 6